WE CLAIM:

1. A computer program product for controlling operation of a computer to detect malware, said computer program product comprising:

(i) pending scan database code operable to maintain a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed; and

(ii) scanning code operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified within said pending scan database.

2. A computer program as claimed in claim 1, further comprising file write code operable as a computer file is written to a storage device to add data identifying said computer file to said pending scan database.

3. A computer program product as claimed in claim 1, further comprising file read code operable in response to a read request for a computer file included within said pending scan database to trigger said scanning code to scan said computer file as a high priority task before permitting read access to said computer file.

4. A computer program product as claimed in claim 1, further comprising scanned file database code operable to maintain a scanned file database storing data identifying computer files that have been scanned for malware.

5. A computer program product as claimed in claim 4, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

6. A computer program product as claimed in claim 5, further comprising file read code operable in response to a read request for a computer file to detected if said computer file is within said scanned file database and a checksum value recalculated for said computer file matches that stored within said scanned file database before permitting said read request.

7. A computer program product as claimed in claim 4, further comprising initiation code operable upon startup to detect any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.

8. A computer program product as claimed in claim 1, wherein said malware comprises one or more of:

(i) a computer file infected with a computer virus;

(ii) a Trojan;

(iii) a banned computer file; and

(iv) a computer file containing banned content.

9. A method for detecting malware, said method comprising the steps of:

(i) maintaining a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed; and

(ii) as a low priority task within a multitasking environment, conducting malware scanning upon computer files identified within said pending scan database.

10. A method as claimed in claim 9, further comprising the step of as a computer file is written to a storage device adding data identifying said computer file to said pending scan database.

11. A method as claimed in claim 9, further comprising the step of in response to a read request for a computer file included within said pending scan database, triggering scanning of said computer file as a high priority task before permitting read access to said computer file.

12. A method as claimed in claim 9, further comprising maintaining a scanned file database storing data identifying computer files that have been scanned for malware.

13. A method as claimed in claim 12, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

14. A method as claimed in claim 13, further comprising the step of in response to a read request for a computer file, detecting if said computer file is within said scanned file database and a checksum value recalculated for said computer file matches that stored within said scanned file database before permitting said read request.

15. A method as claimed in claim 12, further comprising the step of upon startup detecting any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.

16. A method as claimed in claim 9, wherein said malware comprises one or more of:

(i) a computer file infected with a computer virus;

(ii) a Trojan;

(iii) a banned computer file; and

(iv) a computer file containing banned content.

17. Apparatus for detecting malware, said apparatus comprising:

(i) pending scan database logic operable to maintain a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed; and

(ii) a scanner operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified within said pending scan database.

18. Apparatus as claimed in claim 17, further comprising file write logic operable as a computer file is written to a storage device to add data identifying said computer file to said pending scan database.

19. Apparatus as claimed in claim 17, further comprising file read logic operable in response to a read request for a computer file included within said pending scan

database to trigger said scanning logic to scan said computer file as a high priority task before permitting read access to said computer file.

20. Apparatus as claimed in claim 17, further comprising scanned file database logic operable to maintain a scanned file database storing data identifying computer files that have been scanned for malware.

21. Apparatus as claimed in claim 20, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

22. Apparatus as claimed in claim 21, further comprising file read logic operable in response to a read request for a computer file to detected if said computer file is within said scanned file database and a checksum value recalculated for said computer file matches that stored within said scanned file database before permitting said read request.

23. Apparatus as claimed in claim 20, further comprising initiation logic operable upon startup to detect any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.

24. Apparatus as claimed in claim 17, wherein said malware comprises one or more of:

(i) a computer file infected with a computer virus;

(ii) a Trojan;

(iii) a banned computer file; and

(iv) a computer file containing banned content.